USER GUIDE

McAfee® VirusScan® Home Edition

McAfee® SECURITY

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE AGREEMENT

Issued AUGUST 2003 / McAfee® VirusScan® Home Edition software

Contents

Getting Started 1

Welcome to McAfee VirusScan.

McAfee VirusScan is an anti-virus subscription service offering comprehensive, reliable, and up-to-date virus protection. Powered by award-winning McAfee scanning technology, VirusScan protects against viruses, worms, Trojan horses, malicious scripts, and hybrid attacks.

With it, you get the following features:

ActiveShield — Scan files in real-time when they are accessed by either you or your computer.

Scan — Search for viruses in hard drives, floppy disks, and individual files and folders.

Quarantine — Encrypt and temporarily isolate infected and suspicious files in the quarantine folder until an appropriate action can be taken.

Hostile activity detection — Monitor your computer for virus-like activity caused by malicious scripts and worm-like activity.

New features

This version of VirusScan provides the following new features:

- **E-mail scanning**
  VirusScan automatically scans inbound (POP3) and outbound (SMTP) e-mail and e-mail attachments for most popular e-mail clients, including Microsoft Outlook, Netscape Mail, Eudora, and Pegasus.

- **Instant messenger scanning**
  VirusScan automatically scans inbound file transfers for most popular instant messaging clients, including Yahoo Messenger, AOL Instant Messenger, and MSN Messenger.

- **Hostile activity detection**
  VirusScan provides ScriptStopper^{TM} and WormStopper^{TM} to detect, alert, and block virus-like activity caused by malicious scripts and worm-like activity.

- **Windows Explorer integration**
  VirusScan lets you use a shortcut menu to scan selected files, folders, or drives within Windows Explorer.

- **Microsoft Outlook integration**
  VirusScan lets you use a toolbar icon to scan selected messages, folders, or message stores within Microsoft Outlook.

- **Automatic file infection cleaning**
  VirusScan automatically attempts to clean infected files when an infection is detected.

- **Scheduled scanning**
  You can now schedule automatic scanning at specified intervals to thoroughly check your computer for viruses.

- **McAfee SecurityCenter integration**
  Seamless integration with the McAfee SecurityCenter provides a consolidated view of your computer's security status, plus the latest security and virus alerts. You can run SecurityCenter from the McAfee icon in your Windows system tray or from your Windows desktop.

- **File quarantine**
  You can use the Quarantine feature to encrypt and temporarily isolate infected and suspicious files in the quarantine folder until an appropriate action can be taken. Once cleaned, a quarantined file can then be restored to its original location.

- **Submit files to AVERT**
  VirusScan now includes the ability to submit suspicious files directly from the Quarantine feature to the McAfee AntiVirus Emergency Response Team (AVERT™) for research.

- **Virus Map reporting**
  You can now anonymously send virus tracking information for inclusion in our World Virus Map. You can automatically register for this free, secure feature and view the latest worldwide infection rates via the McAfee SecurityCenter.

System requirements

- Microsoft® Windows 98, Windows Me, Windows 2000, or Windows XP
- Personal computer with Pentium 133 MHz or higher processor
- 32 MB of RAM
- 35 MB of free hard disk space (for installation)
- Microsoft® Internet Explorer 5.0 or later

  NOTE
  To upgrade to the latest version of Internet Explorer, visit the Microsoft web site at http://www.microsoft.com/.

Downloading and installing VirusScan

Before you can download and install VirusScan, you must purchase a subscription. To do so, go to the McAfee web site, and create an account with a password and billing information to sign up for the service.

Before installing VirusScan, save all of your work and close any open applications before you continue with the following installation steps. After installing VirusScan, you might be prompted to restart your computer.

> **NOTE**
> If you are upgrading from a previous version of VirusScan, VirusScan automatically uninstalls the previous version before it installs the current version. You must restart your computer if the **Installation Wizard** prompts you. After your computer restarts, the current version of VirusScan installs.

To install VirusScan:

1. Go to http://us.mcafee.com/, and click **My Account**.
2. If prompted, enter your subscribing e-mail address and password, then click **Log In** to open your **Account Info** page.
3. Locate **VirusScan** in **Your Web Services** list, and click the **Update/Download** icon.
4. If any dialog boxes appear, click **Yes** to continue. If the **Installation Wizard** does not appear automatically, click **Start**.

   If the **Installation Wizard** detects other anti-virus software installed on your computer, a list of detected products appears.
5. Click **Yes** (strongly recommended) to remove the detected products, then restart your computer to continue the installation.

   When your computer restarts, the **Installation Wizard** dialog box appears again, prompting you to continue the installation.
6. Click **Next** to continue installing VirusScan.

   The **Virus Map Reporting** dialog box appears.

   a. Accept the default **Yes, I want to participate** option to anonymously send your virus information to McAfee for inclusion in its World Virus Map of worldwide infection rates. Otherwise, select **No, I don't want to participate** to avoid sending your information.

   > **NOTE**
   > You can also configure this option at any time in the **Virus Map Reporting** tab of the **VirusScan Options** dialog box.

b If you are in the United States, select the state and enter the zip code where your computer is located. Otherwise, select the country where your computer is located. When you are finished, click **Next** to continue.

7 If the **Installation Wizard** prompts you, click **Restart** to restart your computer.

A welcome dialog box appears when Windows restarts after the installation.

8 Click **What's New** to read about new product features, then click **Scan for Viruses** to perform an initial scan of your computer for viruses.

The **Scan for Viruses** dialog box appears and begins to perform an initial scan on your computer using the default scanning options. See *Manually scanning for viruses* on page 24 for details.

9 When the scan is finished, click **Close** to exit Scan.

Testing VirusScan

Before initial use of VirusScan, it's a good idea to test your installation. Use the following steps to separately test the ActiveShield and Scan features.

Testing ActiveShield

To test ActiveShield:

1 Go to http://www.eicar.com/ in your web browser.

2 Click the **The AntiVirus testfile eicar.com** link.

3 Scroll to the bottom of the page. Under **Download**, you will see four links.

4 Click **eicar.com**.

If ActiveShield is working properly, it detects the eicar.com file immediately after you click the link. You can try to delete or quarantine infected files to see how ActiveShield handles viruses. See *If ActiveShield finds a virus* on page 21 for details.

Testing Scan

Before you can test Scan, you must download the test files and then move them to another folder.

To download the test files:

1. Disable ActiveShield: Right-click the McAfee icon, point to **VirusScan**, then click **Disable**.

2. Download the EICAR test files from the EICAR web site:

   a. Go to http://www.eicar.com/.

   b. Click the **The AntiVirus testfile eicar.com** link.

   c. Scroll to the bottom of the page. Under **Download**, you will see these links:

      eicar.com contains a line of text that VirusScan will detect as a virus. #*

      eicar.com.txt (optional) is the same file, but with a different file name, for those users who have difficulty downloading the first link. Simply rename the file “eicar.com” after you download it. #*

      eicar_com.zip is a copy of the test virus inside a .ZIP compressed file (a WinZip™ file archive). *

      eicarcom2.zip is a copy of the test virus inside a .ZIP compressed file, which itself is inside a .ZIP compressed file. *

      # The ActiveShield feature detects these file types.

      * The Scan feature detects these file types.

   d. Click each link to download its file. For each one, a **File Download** dialog box appears. Locate a temporary directory, click **Save**, then click **Save** again in each **Save As** dialog box.

3. When you are finished downloading the files, close Internet Explorer.

To move the test files into another folder:

1 In Windows Explorer, double-click the **My Computer** icon.

The **My Computer** window opens.

2 Double-click the icon for your computer's hard drive (usually drive C).

A window opens showing the contents of the hard drive.

3 Right-click an area (not a folder) on the window, point to **New**, then click **Folder**.

A folder named **New Folder** appears.

4 Rename the folder **VSO Scan Folder**.

5 Drag each file from your desktop into the **VSO Scan Folder**.

6 Enable ActiveShield: Right-click the McAfee icon, point to **VirusScan**, then click **Enable**.

To test Scan:

1 Right-click the McAfee icon, point to **VirusScan**, then click **Scan for Viruses**.

2 Using the directory tree in the left pane of the dialog box, go to the **VSO Scan Folder** where you saved the files:

a Click the **+** sign next to the **Primary (C:)** icon.

b Click the **VSO Scan Folder** to highlight it (do not click the **+** sign next to it).

This tells Scan to check only that folder for viruses. You can also put the files in random locations on your hard drive for a more convincing demonstration of Scan’s abilities.

3 In the **Scan Options** area of the **Scan for Viruses** dialog box, ensure that all options are selected.

4 Click **Scan** on the lower right of the dialog box.

VirusScan scans the **VSO Scan Folder**. The files that you saved to that folder will appear in the **List of Infected Files**. If so, Scan is working properly.

You can try to delete or quarantine infected files to see how Scan handles viruses. See *If Scan finds a virus* on page 30 for details.

Using McAfee SecurityCenter

The McAfee SecurityCenter is your one-stop security shop, accessible from its icon in your Windows system tray or from your Windows desktop. With it, you can perform these useful tasks:

- Get free security analysis for your computer.
- Launch, manage, and configure all your McAfee subscriptions from one icon.
- See continuously updated virus alerts and the latest product information.
- Receive free trial subscriptions to download and install trial versions directly from McAfee using our patented software delivery process.
- Get quick links to frequently asked questions and account details at the McAfee web site.

NOTE
For more information about its features, click **Help** in the **SecurityCenter** dialog box.

While the SecurityCenter is running and all of the McAfee features installed on your computer are enabled, a red M icon M appears in the Windows system tray. This area is usually in the lower-right corner of the Windows desktop and contains the clock.

If one or more of the McAfee applications installed on your computer are disabled, the McAfee icon changes to black M.

To open the McAfee SecurityCenter:

1. Right-click the McAfee icon M.
2. Click **Open SecurityCenter**.

To access a VirusScan feature:

1. Right-click the McAfee icon M.
2. Point to **VirusScan**, then click the feature you want to use.

Using McAfee VirusScan 2

Using ActiveShield

When ActiveShield is started (loaded into computer memory) and enabled, it is constantly protecting your computer. ActiveShield scans files when they are accessed by either you or your computer. When ActiveShield detects an infected file, it automatically tries to clean the virus. If ActiveShield cannot clean the virus, you can quarantine or delete the file.

WARNING

- VirusScan and ActiveShield are not upgrades from McAfee VirusScan v4.x–7.x and VShield. If you have McAfee VirusScan on your computer, you must remove it so ActiveShield runs correctly.
- Software packages such as McAfee Internet Security, Guard Dog, Nuts & Bolts, First Aid, McAfee Office, and Microsoft Plus! might have versions of McAfee VirusScan bundled with them. You must remove the anti-virus components from these applications before ActiveShield can function properly.

Enabling or disabling ActiveShield

ActiveShield is started (loaded into computer memory) and enabled (denoted by red M) by default as soon as you restart your computer after the installation process.

If ActiveShield is stopped (not loaded) or is disabled (denoted by black M), you can manually run it, as well as configure it to start automatically when Windows starts.

Enabling ActiveShield

To enable ActiveShield for this Windows session only:

Right-click the McAfee icon, point to **VirusScan**, then click **Enable**. The McAfee icon changes to red M.

If ActiveShield is still configured to start when Windows starts, a message tells you that you are now protected from viruses. Otherwise, a dialog box appears that lets you configure ActiveShield to start when Windows starts (Figure 2-1 on page 14).

Disabling ActiveShield

To disable ActiveShield for this Windows session only:

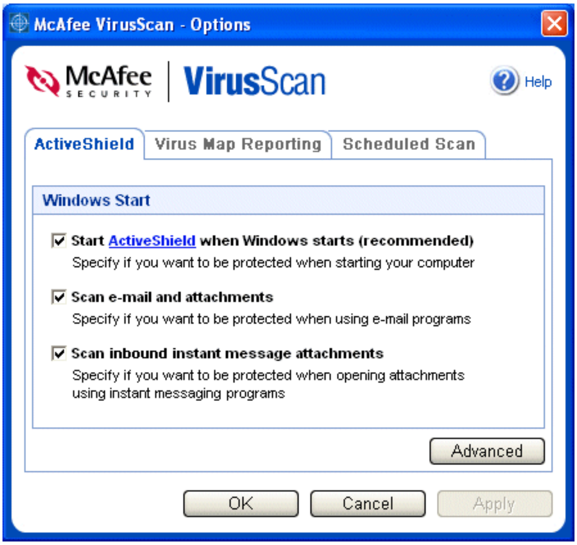
1. Right-click the McAfee icon, point to **VirusScan**, then click **Disable**.
2. Click **Yes** to confirm.

   The McAfee icon changes to black M.

If ActiveShield is still configured to start when Windows starts, your computer will be protected from viruses again when you restart your computer.

Configuring ActiveShield options

You can modify ActiveShield starting and scanning options in the **ActiveShield** tab of the **VirusScan Options** dialog box (Figure 2-1), which is accessible via the McAfee icon M in your Windows system tray.



☑ Start ActiveShield when Windows starts (recommended)
Specify if you want to be protected when starting your computer

☑ Scan e-mail and attachments
Specify if you want to be protected when using e-mail programs

☑ Scan inbound instant message attachments
Specify if you want to be protected when opening attachments using instant messaging programs

Figure 2-1. ActiveShield Options

Starting ActiveShield

ActiveShield is started (loaded into computer memory) and enabled (denoted by red M) by default as soon as you restart your computer after the installation process.

If ActiveShield is stopped (denoted by black M), you can configure it to start automatically when Windows starts (recommended).

NOTE
During updates to VirusScan, the **Update Wizard** might exit ActiveShield temporarily to install new files. When the **Update Wizard** prompts you to click **Finish**, ActiveShield starts again.

To start ActiveShield automatically when Windows starts:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.

   The **VirusScan Options** dialog box opens (Figure 2-1 on page 14).

2. Select the **Start ActiveShield when Windows starts (recommended)** checkbox, then click **Apply** to save your changes.

3. Click **OK** to confirm, then click **OK**.

Stopping ActiveShield

WARNING
If you stop ActiveShield, your computer is not protected from viruses. If you must stop ActiveShield, other than for updating VirusScan, ensure that you are not connected to the Internet.

To stop ActiveShield from starting when Windows starts:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.

   The **VirusScan Options** dialog box opens (Figure 2-1 on page 14).

2. Deselect the **Start ActiveShield when Windows starts (recommended)** checkbox, then click **Apply** to save your changes.

3. Click **OK** to confirm, then click **OK**.

Scanning e-mail and attachments

By default, e-mail scanning and automatic cleaning are enabled via the **Scan e-mail and attachments** option (Figure 2-1 on page 14) and the **Automatically clean infected attachments (recommended)** option (Figure 2-2 on page 17).

When these two options are enabled, ActiveShield automatically scans and attempts to clean inbound (POP3) and outbound (SMTP) infected e-mail messages and attachments for most popular e-mail clients, including the following:

- Microsoft Outlook Express 4.0 or later
- Microsoft Outlook 97 or later
- Netscape Messenger 4.0 or later
- Netscape Mail 6.0 or later

- Eudora Light 3.0 or later
- Eudora Pro 4.0 or later
- Eudora 5.0 or later
- Pegasus 4.0 or later

NOTE
E-mail scanning is not supported for these e-mail clients: Web-based, IMAP, AOL, POP3 SSL, and Lotus Notes. However, ActiveShield scans e-mail attachments when they are opened.

Inbound e-mail

If an inbound e-mail message or attachment is infected, ActiveShield performs the following steps:

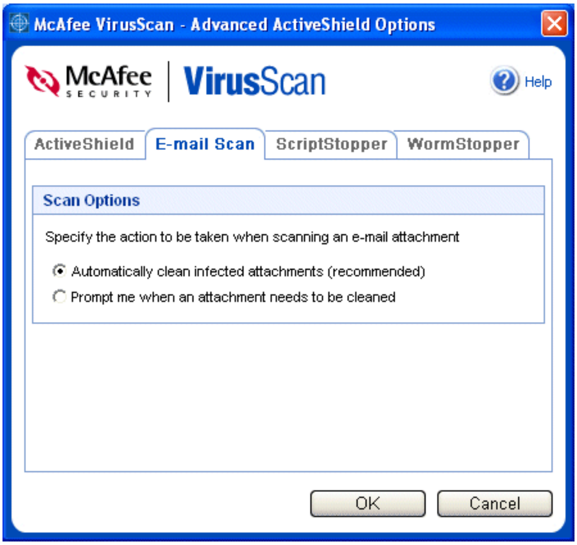
- Tries to clean the infected e-mail
- Tries to quarantine or delete an uncleanable e-mail
- Includes an alert file in the inbound e-mail that contains information about the actions performed to remove the infection

Outbound e-mail

If an outbound e-mail message or attachment is infected, ActiveShield performs the following steps:

- Tries to clean the infected e-mail
- Tries to quarantine or delete an uncleanable e-mail
- Sends an alert file to you in a new e-mail that contains information about the actions performed to remove the infection

If your e-mail server is set to only send and receive e-mail while you are at your computer, you can choose to have alerts prompt you to clean infected e-mail by disabling auto-cleaning. Follow the steps below to disable auto-cleaning, then see *Managing infected e-mail* on page 22 for details about responding to alerts.



Scan Options

Specify the action to be taken when scanning an e-mail attachment

● Automatically clean infected attachments (recommended)

○ Prompt me when an attachment needs to be cleaned

Figure 2-2. E-mail Scan Options

To disable auto-cleaning of infected e-mail:

1. Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
2. Click **Advanced**, then click the **E-mail Scan** tab (Figure 2-2).
3. Click **Prompt me when an attachment must be cleaned**, then click **OK**.

Scanning inbound instant message attachments

By default, scanning of instant message attachments is enabled via the **Scan inbound instant message attachments** option (Figure 2-1 on page 14).

When this option is enabled, VirusScan automatically scans and attempts to clean inbound infected instant message attachments for most popular instant messaging clients, including the following:

- MSN Messenger 6.0 or later
- Yahoo Messenger 4.1 or later
- AOL Instant Messenger 2.1 or later

NOTE
For your protection, you cannot disable auto-cleaning of instant message attachments.

If an inbound instant message attachment is infected, VirusScan performs the following steps:

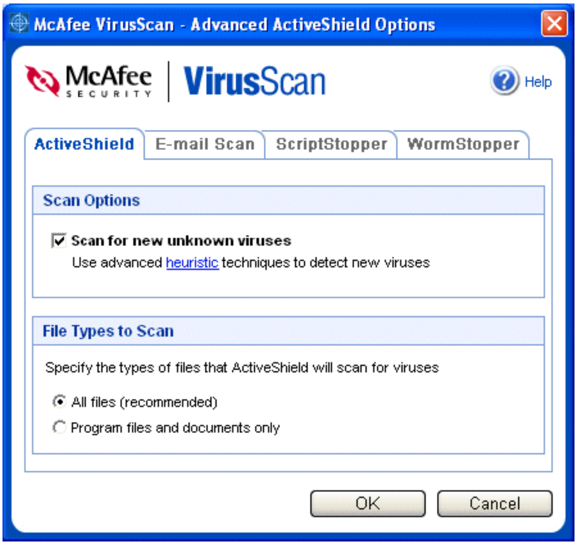
- Tries to clean the infected message
- Prompts you to quarantine or delete an uncleanable message

Scanning all files

If you set ActiveShield to use the default **All files (recommended)** option, it scans every file type that your computer uses, as your computer attempts to use it. Use this option to get the most thorough scan possible.

To set ActiveShield to scan all file types:

1. Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
2. Click **Advanced**, then click the **ActiveShield** tab (Figure 2-3).
3. Click **All files (recommended)**, then click **OK**.



☑ Scan for new unknown viruses

Use advanced heuristic techniques to detect new viruses

Specify the types of files that ActiveShield will scan for viruses

● All files (recommended)

○ Program files and documents only

Figure 2-3. Advanced ActiveShield Options

Scanning program files and documents only

If you set ActiveShield to use the **Program files and documents only** option, it scans program files and documents, but not any other files used by your computer. The latest virus signature file (DAT file) determines which file types that ActiveShield will scan.

To set ActiveShield to scan program files and documents only:

1. Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
2. Click **Advanced**, then click the **ActiveShield** tab (Figure 2-3).
3. Click **Program files and documents only**, then click **OK**.

Scanning for new unknown viruses

If you set ActiveShield to use the default **Scan for new unknown viruses (recommended)** option, it uses advanced heuristic techniques that try to match files to the signatures of known viruses, while also looking for telltale signs of unidentified viruses in the files.

To set ActiveShield to scan for new unknown viruses:

1. Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
2. Click **Advanced**, then click the **ActiveShield** tab (Figure 2-3 on page 18).
3. Click **Scan for new unknown viruses (recommended)**, then click **OK**.

Scanning for scripts and worms

VirusScan monitors your computer for suspicious activity that might indicate a threat is present on your computer. While VirusScan cleans viruses, ScriptStopper^{TM} and WormStopper^{TM} prevent viruses, worms, and Trojans from spreading further.

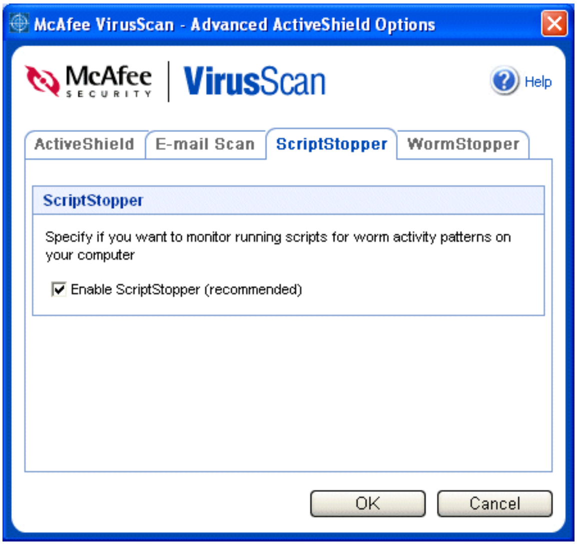
The ScriptStopper and WormStopper protection mechanisms detect, alert, and block malicious activity. Suspicious activity might include the following actions on your computer:

- A script execution that results in the creation, copying, or deletion of files, or the opening of your Windows registry
- An attempt to forward e-mail to a large portion of your address book
- Attempts to forward multiple e-mail messages in rapid succession

If you set ActiveShield to use the default **Enable ScriptStopper (recommended)** and **Enable WormStopper (recommended)** options in the **Advanced Options** dialog box, ScriptStopper and WormStopper monitor script execution and e-mail activity for suspicious patterns and alerts you when a specified number of e-mails or recipients has been exceeded within a specified interval.

To set ActiveShield to scan for malicious scripts and worm-like activity:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.
2. Click **Advanced**, click the **ScriptStopper** tab, then click **Enable ScriptStopper (recommended)** (Figure 2-4 on page 20).



ScriptStopper

Specify if you want to monitor running scripts for worm activity patterns on your computer

☑ Enable ScriptStopper (recommended)

Figure 2-4. ScriptStopper Options

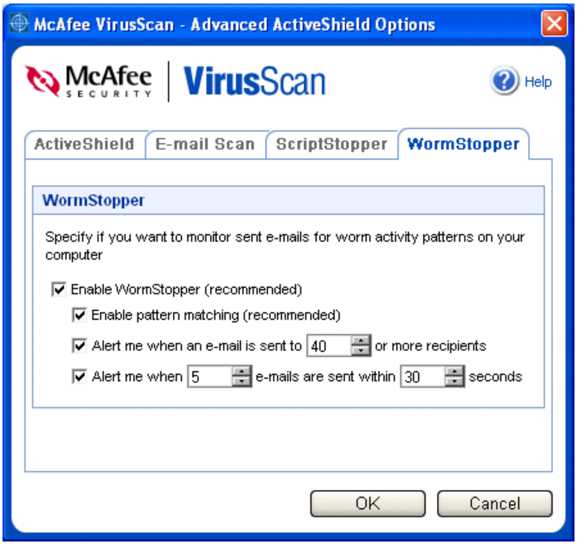
3 Click the **WormStopper** tab, click **Enable WormStopper (recommended)**, then click **OK** (Figure 2-5 on page 21).

By default, the following detailed options are enabled:

- Pattern matching to detect suspicious activity
- Alerting when e-mail is sent to 40 or more recipients
- Alerting when 5 or more e-mails are sent within 30 seconds

This option can be automatically enabled after the first time a potential worm is detected (see *Managing potential worms* on page 23 for details):

- Automatic blocking of suspicious outbound e-mails



WormStopper

Specify if you want to monitor sent e-mails for worm activity patterns on your computer

☑ Enable WormStopper (recommended)

☑ Enable pattern matching (recommended)

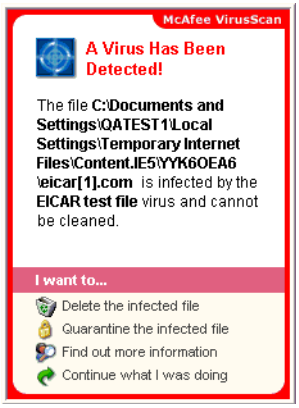
☑ Alert me when an e-mail is sent to 40 or more recipients

☑ Alert me when 5 e-mails are sent within 30 seconds

Figure 2-5. WormStopper Options

If ActiveShield finds a virus

If ActiveShield finds a virus, a virus alert similar to Figure 2-6 appears. For most viruses, Trojan horses, and worms, ActiveShield automatically tries to clean the file. You can then choose how to manage infected files, infected e-mail, suspicious scripts, and potential worms, and whether to submit infected files to the McAfee AVERT labs for research.



A Virus Has Been Detected!

The file **C:\Documents and Settings\QATEST1\Local Settings\Temporary Internet Files\Content.IE5\YYK6OEA6\eicar[1].com** is infected by the **EICAR test file** virus and cannot be cleaned.

I want to...

- Delete the infected file
- Quarantine the infected file
- Find out more information
- Continue what I was doing

Figure 2-6. Virus Alert

Managing infected files

1. If ActiveShield can clean the file, you can learn more or ignore the alert:

    - Click **Find out more information** to view the name, location, and virus name associated with the infected file.

    - Click **Continue what I was doing** to ignore the alert and close it.

2. If ActiveShield cannot clean the file, click **Quarantine the infected file** to encrypt and temporarily isolate infected and suspicious files in the quarantine directory until an appropriate action can be taken.

    A confirmation message appears and prompts you to check your computer for viruses. Click **Scan** to complete the quarantine process.

3. If ActiveShield cannot quarantine the file, click **Delete the infected file** to try to remove the file.

Managing infected e-mail

1. If you disabled auto-cleaning of e-mail, you can learn more and clean the e-mail:

    a. Click **Find out more information** to view the file name, virus name, infection status, sender, and subject associated with the infected e-mail.

    b. Click **Clean the infected attachment**.

2. If ActiveShield cannot clean the e-mail, click **Quarantine the infected attachment** to encrypt and temporarily isolate infected and suspicious files in the quarantine directory until an appropriate action can be taken.

    A confirmation message appears and prompts you to check your computer for viruses. Click **Scan** to complete the quarantine process.

3. If ActiveShield cannot quarantine the e-mail, click **Delete the infected attachment** to try to remove the file.

Managing suspicious scripts

1 If ActiveShield detects a suspicious script, you can find out more and then stop the script if you did not intend to initiate it:

   a Click **Find out more information** to view the name, location, and description of the activity associated with the suspicious script.

   b Click **Stop this script** to prevent the suspicious script from running.

2 If you are sure that you trust the script, you can allow the script to run:

   a Click **Allow all scripts this time** to let all scripts contained within a single file to run once.

   b Click **Continue what I was doing** to ignore the alert and let the script run.

Managing potential worms

1 If ActiveShield detects a potential worm, you can find out more and then stop the e-mail activity if you did not intend to initiate it:

   a Click **Find out more information** to view the recipient list, subject line, message body, and description of the suspicious activity associated with the infected e-mail message.

   b Click **Stop this e-mail** to prevent the suspicious e-mail from being sent and delete it from your message queue.

      NOTE
      The first time a potential worm is detected, a dialog box appears after you either stop or send the suspicious e-mail. Select the **Automatically block all suspicious outbound e-mails** checkbox, then click **OK** to configure WormStopper to silently block the sending of suspicious e-mail in the future.

2 If you are sure that you trust the e-mail activity, click **Continue what I was doing** to ignore the alert and let the e-mail be sent.

Scanning your computer for viruses

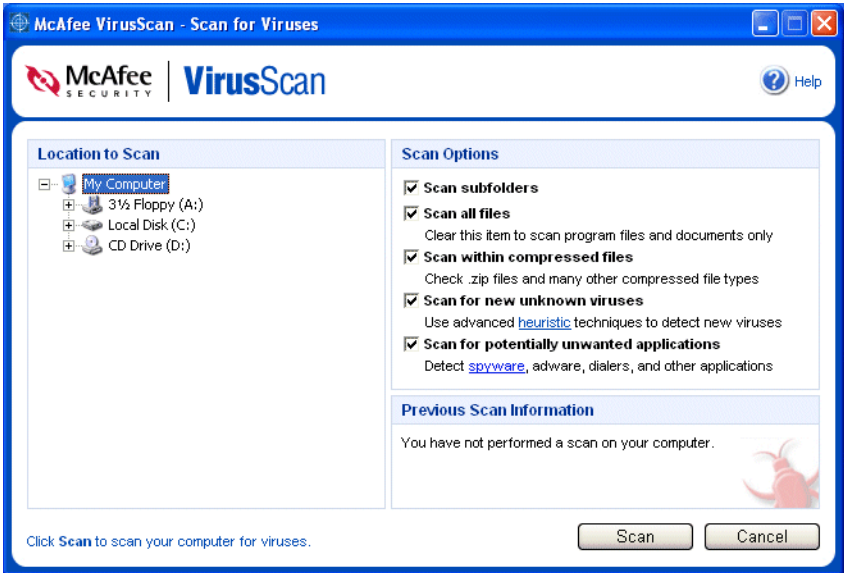
The Scan feature lets you selectively search for viruses on hard drives, floppy disks, and individual files and folders. When Scan finds an infected file, it automatically tries to clean the file. If Scan cannot clean the virus, you can quarantine or delete the file.

Manually scanning for viruses

To scan your computer:

1 Right-click the McAfee icon, point to **VirusScan**, then click **Scan for Viruses**.

The **Scan for Viruses** dialog box opens (Figure 2-7 on page 24).



☑ Scan subfolders

☑ Scan all files

Clear this item to scan program files and documents only

☑ Scan within compressed files

Check .zip files and many other compressed file types

☑ Scan for new unknown viruses

Use advanced heuristic techniques to detect new viruses

☑ Scan for potentially unwanted applications

Detect spyware, adware, dialers, and other applications

You have not performed a scan on your computer.

Click **Scan** to scan your computer for viruses.

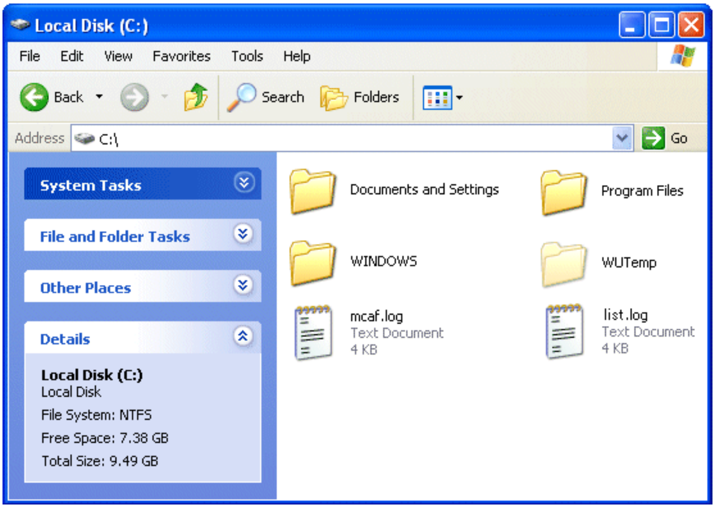
Figure 2-7. Scan for Viruses

2 Click the drive, folder, or file that you want to scan.

3 Select your **Scan Options**. By default, all of the **Scan Options** are pre-selected to provide the most thorough scan possible (Figure 2-7):

- **Scan subfolders** — Use this option to scan files contained in your subfolders. Deselect this checkbox to allow checking of only the files visible when you open a folder or drive.

  Example: The files in Figure 2-8 on page 25 are the only files scanned if you deselect the **Scan subfolders** checkbox. The folders and their contents are not scanned. To scan those folders and their contents, you must leave the checkbox selected.



Local Disk (C:)
Local Disk
File System: NTFS
Free Space: 7.38 GB
Total Size: 9.49 GB

Figure 2-8. Local Disk Contents

- **Scan all files** — Use this option to allow the thorough scanning of all file types. Deselect this checkbox to shorten the scanning time and allow checking of program files and documents only.

- **Scan within compressed files** — Use this option to reveal hidden infected files within .ZIP and other compressed files. Deselect this checkbox to prevent checking of any files or compressed files within the compressed file.

  Sometimes virus authors plant viruses in a .ZIP file, then insert that .ZIP file into another .ZIP file in an effort to bypass anti-virus scanners. Scan can detect these viruses as long as you leave this option selected.

- **Scan for new unknown viruses** — Use this option to find the newest viruses that might not have existing “cures.” This option uses advanced heuristic techniques that try to match files to the signatures of known viruses, while also looking for telltale signs of unidentified viruses in the files.

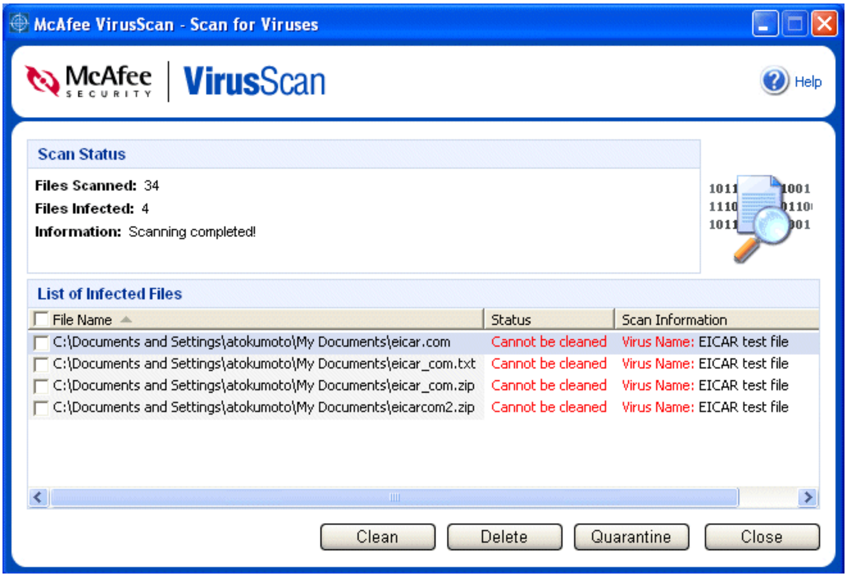
  This scanning method also looks for file traits that can generally rule out that the file contains a virus. This minimizes the chances that Scan gives a false indication. Nevertheless, if a heuristic scan detects a virus, you should treat it with the same caution that you would treat a file that you know contains a virus.

  This option provides the most thorough scan, but is generally slower than a normal scan.

- **Scan for potentially unwanted applications** — Use this option to detect spyware, adware, dialers, and other applications that you did not intent to install on your computer.

  NOTE
  Leave all options selected for the most thorough scan possible. This effectively scans every file in the drive or folder that you select, so allow plenty of time for the scan to complete. The larger the hard drive and the more files you have, the longer the scan takes.

4 Click **Scan** to start scanning files. When the scan is finished, a list of any infected files appears in the **Scan for Viruses** dialog box (Figure 2-9).



Scan Status

Files Scanned: 34
Files Infected: 4
Information: Scanning completed!

List of Infected Files

□ File Name	Status	Scan Information
□ C:\Documents and Settings\atokumoto\My Documents\eicar.com	Cannot be cleaned	Virus Name: EICAR test file
□ C:\Documents and Settings\atokumoto\My Documents\eicar_com.txt	Cannot be cleaned	Virus Name: EICAR test file
□ C:\Documents and Settings\atokumoto\My Documents\eicar_com.zip	Cannot be cleaned	Virus Name: EICAR test file
□ C:\Documents and Settings\atokumoto\My Documents\eicarcom2.zip	Cannot be cleaned	Virus Name: EICAR test file

Figure 2-9. Scan Results

NOTE
Scan counts a compressed file (.ZIP, .CAB, etc.) as one file within the **Files Scanned** number. Also, the number of files scanned can vary if you have deleted your temporary Internet files since your last scan.

5 If Scan finds no viruses, click **Back** to select another drive or folder to scan, or click **Close** to close the dialog box.

Scanning for viruses in Windows Explorer

VirusScan lets you use a shortcut menu to scan selected files, folders, or drives from within Windows Explorer.

To scan files in Windows Explorer:

1. Open Windows Explorer.
2. Right-click the drive, folder, or file that you want to scan, and then click **Scan for Viruses**.

   The **Scan for Viruses** dialog box opens and starts scanning files. By default, all of the default **Scan Options** are pre-selected to provide the most thorough scan possible (Figure 2-7 on page 24).

Scanning for viruses in Microsoft Outlook

VirusScan lets you use a toolbar icon to scan selected message stores and their subfolders, mailbox folders, or e-mail messages containing attachments within Microsoft Outlook 97 or later.

To scan e-mail in Microsoft Outlook:

1. Open Microsoft Outlook.
2. Click the message store, folder, or e-mail message containing an attachment that you want to scan, and then click the e-mail scanning toolbar icon.

   The e-mail scanner opens and starts scanning files. By default, all of the default **Scan Options** are pre-selected to provide the most thorough scan possible (Figure 2-7 on page 24).

Automatically scanning for viruses

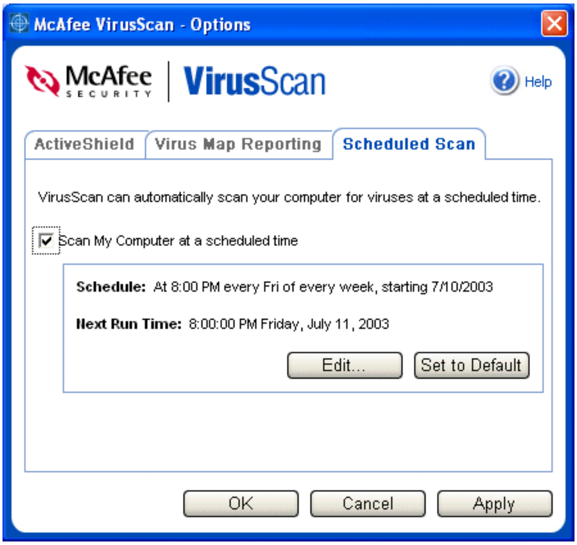
Although VirusScan scans files when they are accessed by either you or your computer, you can schedule automatic scanning in **Windows Scheduler** to thoroughly check your computer for viruses at specified intervals.

To schedule a scan:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.

   The **VirusScan Options** dialog box opens.

2. Click the **Scheduled Scan** tab (Figure 2-10 on page 28).



VirusScan can automatically scan your computer for viruses at a scheduled time.

☑ Scan My Computer at a scheduled time

Schedule: At 8:00 PM every Fri of every week, starting 7/10/2003

Next Run Time: 8:00:00 PM Friday, July 11, 2003

Figure 2-10. Scheduled Scan Options

3 Select the **Scan My Computer at a scheduled time** checkbox to enable automatic scanning.

4. Define a schedule for automatic scanning using either of the following methods:

   - To accept the default schedule (**8PM every Friday**), click **OK**.
   - To edit a schedule:

     a. Click **Edit**.

     b. Select the schedule in the list.

     c. Select how often to scan your computer in the **Frequency** list, then select additional options in the dynamic area below it:

        Daily — Specify the number of days between scans.

        Weekly (the default) — Specify the number of weeks between scans as well as the names of the day(s) of the week.

        Monthly — Specify which day of the month to scan. Click **Select Months** to specify which months to scan, and click **OK**.

        Once — Specify which date to scan.

        At user logon — Select to automatically scan your computer every time a user logs on to your computer.

        > **NOTE**
        > These options in Windows Scheduler are not supported: **At system startup**, **When idle**, and **Show multiple schedules**. The last supported schedule remains enabled until you select from among the valid options.

     d. Select the time of day to scan your computer in the **Start time** box.

     e. To select advanced options, click **Advanced.** The **Advanced Schedule Options** dialog box opens.

        Specify a start date, end date, duration, end time, and whether to stop the task at the specified time if the scan is still running.

        Click **OK** to save your changes and close the dialog box. Otherwise, click **Cancel**.

5. Click **OK** to save your changes and close the dialog box. Otherwise, click **Cancel**.

6. To revert to the default schedule, click **Set to Default**. Otherwise, click **OK**.

If Scan finds a virus

For most viruses, Trojans, and worms, Scan automatically tries to clean the file. You can then choose how to manage infected files, including whether to submit them to the McAfee AVERT labs for research.

If Scan cannot clean the virus, you can quarantine or delete the file:

1. If a file appears in the list of infected files, click the checkbox in front of the file to select it.

   NOTE
   If more than one file appears in the list, you can select the checkbox in front of the **File Name** list to perform the same action on all of the files. You can also click the virus name in the **Virus** list to view details from the Virus Information Library.

2. If Scan cannot clean the virus, you can click **Quarantine** to encrypt and temporarily isolate infected and suspicious files in the quarantine directory until an appropriate action can be taken. (See *Managing quarantined files* for details.)

3. If Scan cannot clean or quarantine the file, you can do either of the following:

   - Click **Delete** to remove the file.
   - Click **Cancel** to close the dialog box without taking any further action.

If Scan cannot clean or delete the virus, consult the Virus Information Library at http://mast.mcafee.com/default.asp for instructions on manually deleting the virus.

If the virus prevents you from using your Internet connection or from using your computer at all, try using a Rescue Disk to start your computer. The Rescue Disk, in many cases, can start a computer if a virus disables it. See *Creating a Rescue Disk* on page 32 for details.

For more help, consult McAfee Customer Support at http://mcafeehelp.com/.

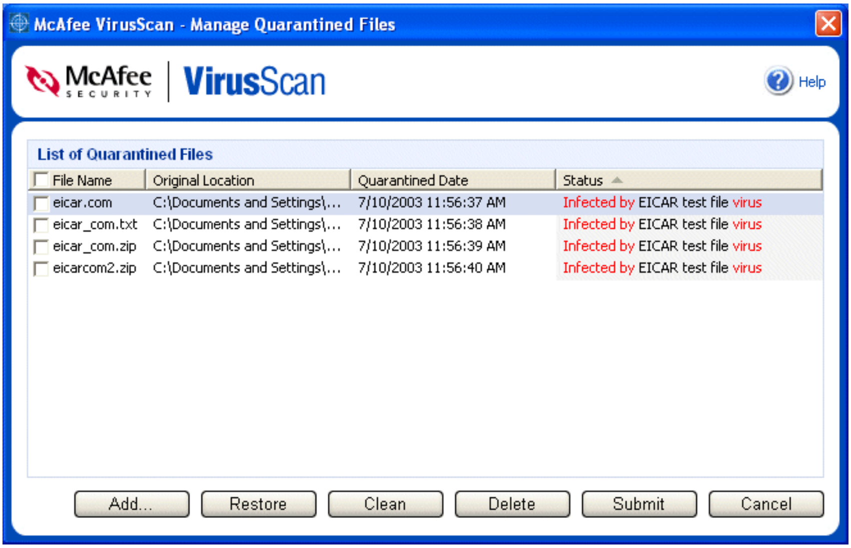
Managing quarantined files

The Quarantine feature encrypts and temporarily isolates infected and suspicious files in the quarantine directory until an appropriate action can be taken. Once cleaned, a quarantined file can then be restored to its original location.

To manage a quarantined file:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Manage Quarantined Files**.

   A list of quarantined files appears (Figure 2-11 on page 31).



List of Quarantined Files

☐ File Name	Original Location	Quarantined Date	Status
☐ eicar.com	C:\Documents and Settings\...	7/10/2003 11:56:37 AM	Infected by EICAR test file virus
☐ eicar_com.txt	C:\Documents and Settings\...	7/10/2003 11:56:38 AM	Infected by EICAR test file virus
☐ eicar_com.zip	C:\Documents and Settings\...	7/10/2003 11:56:39 AM	Infected by EICAR test file virus
☐ eicarcom2.zip	C:\Documents and Settings\...	7/10/2003 11:56:40 AM	Infected by EICAR test file virus

Figure 2-11. Manage Quarantined Files

2 Select the checkbox next to the file(s) you want to clean.

> **NOTE**
> If more than one file appears in the list, you can select the checkbox in front of the **File Name** list to perform the same action on all of the files. You can also click the virus name in the **Status** list to view details from the Virus Information Library.

Or, click **Add**, select a suspicious file to add to the quarantine list, click **Open**, then select it in the quarantine list.

3 Click **Clean**.

4 If the file is cleaned, click **Restore** to move it back to its original location.

5 If VirusScan cannot clean the virus, click **Delete** to remove the file.

6 If VirusScan cannot clean or delete the file, you can submit the file to the McAfee AntiVirus Emergency Response Team (AVERT^{TM}) for research:

   a Update your virus signature files if they are more than two weeks old.

   b Verify your subscription.

c Select the file and click **Submit** to submit the file to AVERT.

VirusScan sends the quarantined file as an attachment with an e-mail message containing your e-mail address, country, software version, OS, and the file's original name and location. The maximum submission size is one unique 1.5-MB file per day.

7 Click **Cancel** to close the dialog box without taking any further action.

Creating a Rescue Disk

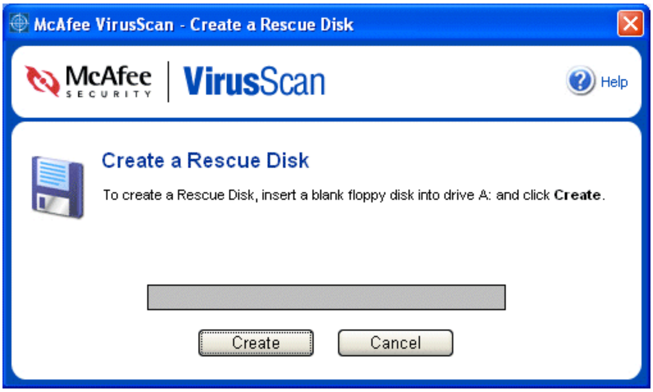
Rescue Disk is a utility that creates a bootable floppy disk that you can use to start your computer and scan it for viruses if a virus keeps you from starting it normally.

NOTE
You must be connected to the Internet to download the Rescue Disk image. Also, Rescue Disk is available for computers with FAT (FAT 16 and FAT 32) hard drive partitions only. It is unnecessary for NTFS partitions.

To create a Rescue Disk:

1. On a non-infected computer, insert a non-infected floppy disk in drive A. You might want to use Scan to ensure that both the computer and the floppy disk are virus-free. (See *Manually scanning for viruses* on page 24 for details.)
2. Right-click the McAfee icon, point to **VirusScan**, then click **Create Rescue Disk**.

   The **Create a Rescue Disk** dialog box opens (Figure 2-12).



Create a Rescue Disk

To create a Rescue Disk, insert a blank floppy disk into drive A: and click **Create**.

Figure 2-12. Create a Rescue Disk

3 Click **Create** to create the Rescue Disk.

If this is your first time creating a Rescue Disk, a message tells you that Rescue Disk needs to download the image file for the Rescue Disk. Click **OK** to download the component now, or click **Cancel** to download it later.

A warning message tells you that the contents of the floppy disk will be lost.

4 Click **Yes** to continue creating the Rescue Disk.

The creation status appears in the **Create Rescue Disk** dialog box.

5 When the message "Rescue disk created" appears, click **OK**, then close the **Create Rescue Disk** dialog box.

6 Remove the Rescue Disk from the drive, write-protect it, and store it in a safe location.

Write-protecting a Rescue Disk

To write-protect a Rescue Disk:

1 Turn the floppy disk label-side down (the metal circle should be visible).

2 Locate the write-protect tab. Slide the tab so the hole is visible.

Using a Rescue Disk

To use a Rescue Disk:

1 Turn off the infected computer.

2 Insert the Rescue Disk into the drive.

3 Turn the computer on.

A gray window with several options appears.

4 Choose the option that best suits your needs by pressing the Function keys (for example, F2, F3).

> **NOTE**
> Rescue Disk starts automatically in 60 seconds if you do not press any of the keys.

Updating a Rescue Disk

It is a good idea to update your Rescue Disk regularly. To update your Rescue Disk, follow the same instructions for creating a new Rescue Disk.

Automatically reporting viruses

You can anonymously send virus tracking information for inclusion in our World Virus Map. Automatically register for this free, secure feature either during VirusScan installation (in the **Virus Map Reporting** dialog box), or at any time in the **Virus Map Reporting** tab of the **VirusScan Options** dialog box.

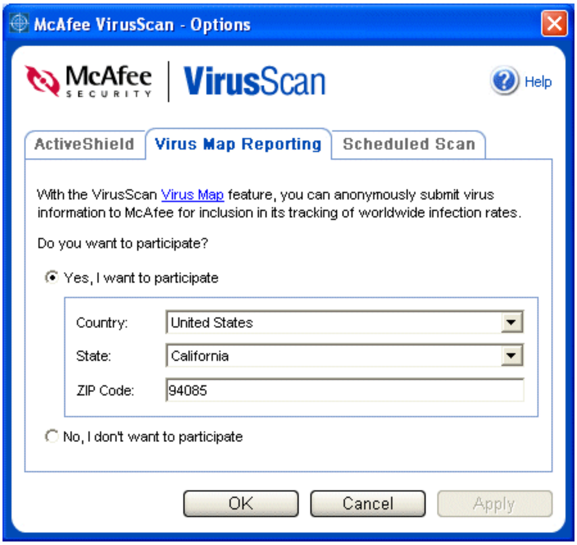
Reporting to the World Virus Map

To automatically report virus information to the World Virus Map:

1 Right-click the McAfee icon, point to **VirusScan**, then click **Options**.

The **VirusScan Options** dialog box opens.

2 Click the **Virus Map Reporting** tab (Figure 2-13).



With the VirusScan Virus Map feature, you can anonymously submit virus information to McAfee for inclusion in its tracking of worldwide infection rates.

Do you want to participate?

● Yes, I want to participate

Country: United States

State: California

ZIP Code: 94085

○ No, I don't want to participate

Figure 2-13. Virus Map Reporting Options

3 Accept the default **Yes, I want to participate** to anonymously send your virus information to McAfee for inclusion in its World Virus Map of worldwide infection rates. Otherwise, select **No, I don't want to participate** to avoid sending your information.

4 If you are in the United States, select the state and enter the zip code where your computer is located. Otherwise, VirusScan automatically tries to select the country where your computer is located.

5 Click **OK**.

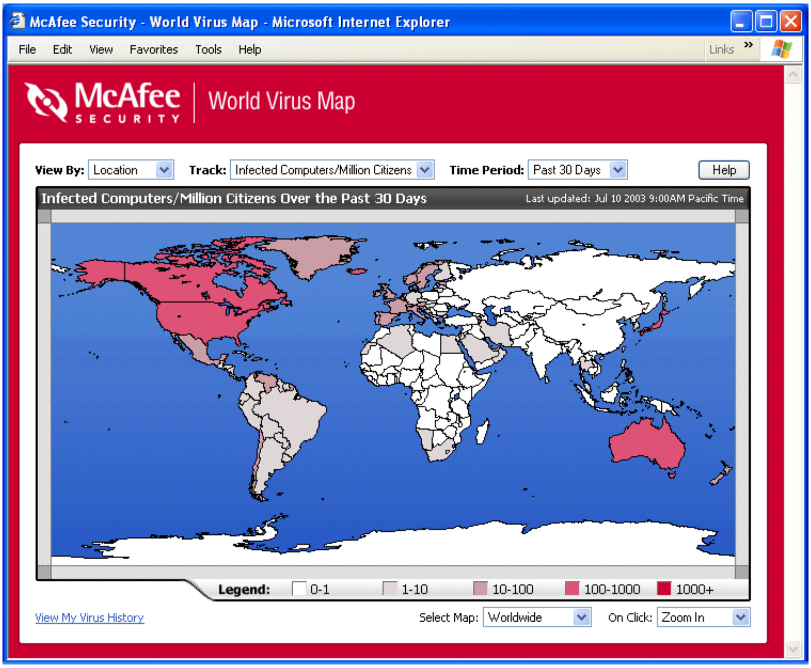
Viewing the World Virus Map

Whether or not you participate in the World Virus Map, you can view the latest worldwide infection rates via the McAfee icon in your Windows system tray.

To view the World Virus Map:

- Right-click the McAfee icon, point to **VirusScan**, then click **World Virus Map**.

  The **World Virus Map** web page appears (Figure 2-14).



McAfee Security - World Virus Map - Microsoft Internet Explorer

View By: Location
Track: Infected Computers/Million Citizens
Time Period: Past 30 Days

Infected Computers/Million Citizens Over the Past 30 Days
Last updated: Jul 10 2003 9:00AM Pacific Time

Legend: □ 0-1 □ 1-10 □ 10-100 □ 100-1000 □ 1000+

Select Map: Worldwide
On Click: Zoom In

Figure 2-14. World Virus Map

By default, the World Virus Map shows the number of infected computers worldwide over the past 30 days, and also when the reporting data was last updated. You can change the map view to show the number of infected files, or change the time period to show only the results over the past 7 days or the past 24 hours.

The **Virus Tracking** section lists cumulative totals for the number of scanned files, infected files, and infected computers that have been reported since the date shown.

Updating VirusScan

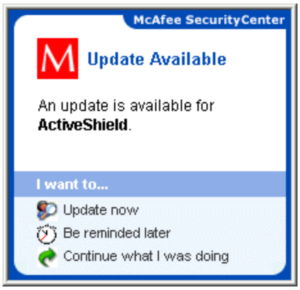
When you are connected to the Internet, VirusScan automatically checks for updates every four hours, then automatically downloads and installs weekly virus definition updates without interrupting your work.

Virus definition files are approximately 100 KB and thus have minimal impact on system performance during download.

If a product update or virus outbreak occurs, an alert appears. Once alerted, you can then choose to update VirusScan to remove the threat of a virus outbreak.

Automatically checking for updates

You must be connected to the Internet for VirusScan to check for available updates. If an update is available, an alert appears (similar to Figure 2-15).



Update Available

An update is available for **ActiveShield**.

Figure 2-15. Update Alert

To update VirusScan:

1. Click **Update now** on the **Update Available** alert (Figure 2-15).
2. Log on to the McAfee web site if VirusScan prompts you to do so. The update downloads automatically.
3. Click **Finish** on the **Completing the VirusScan Wizard** dialog box when the update is finished installing.

> **NOTE**
> In some cases, you will be prompted to restart your computer to complete the update. Be sure to save all of your work and close all applications before restarting.

If you are too busy to update VirusScan when the alert appears, you can postpone updating by doing either of the following:

- Click **Be reminded later** on the **Update Available** alert (Figure 2-15 on page 36), select a time delay for your next update reminder, then click **OK**. You can select from 10 minutes, 20 minutes, 30 minutes, 1 hour, 2 hours, or 4 hours (the default).
- Click **Continue what I was doing** to close the alert without taking any action.

Manually checking for updates

In addition to automatically checking for updates every four hours when you are connected to the Internet, you can also manually check for updates at any time.

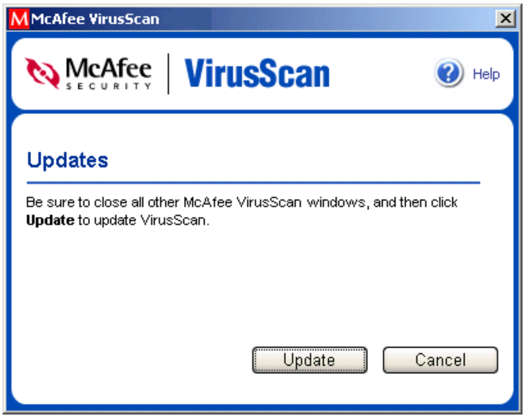
To manually check for VirusScan updates:

1. Ensure your computer is connected to the Internet.
2. Right-click the McAfee icon, then click **Updates**.

   The **SecurityCenter Updates** dialog box opens.
3. Click **Check Now**.

   If an update exists, the **VirusScan Updates** dialog box opens (Figure 2-16). Click **Update** to continue.

   If no updates are available, a dialog box tells you that VirusScan is up-to-date. Click **OK** to close the dialog box.



Be sure to close all other McAfee VirusScan windows, and then click **Update** to update VirusScan.

Figure 2-16. Updates Dialog Box

4. Log on to the web site if prompted. The **Update Wizard** installs the update automatically.

5 Click **Finish** when the update is finished installing.

NOTE
In some cases, you will be prompted to restart your computer to complete the update. Be sure to save all of your work and close all applications before restarting.

Index